REMARKS

Claims 34, 36-49, 51-64, and 66-78 are presented for examination. Claims 34, 36, 37, 49, 51, 64, and 66 are amended herein to more distinctly claimed subject matter which the Applicants regard as the invention. No new matter has been introduced into the application by these amendments.

Claim Rejections - 35 USC § 101

Claims 49, and 51-63 stand rejected under 35 USC § 101 as being allegedly directed to non-statutory subject matter as failing to fall within a statutory category and as being directed to software per se. The rejection is not understood. The rejected claims each recite an apparatus comprising means for performing certain recited functions. Such claims are in a means-plus-function form that is statutorily permitted. 35 USC 112, paragraph 6, states: "An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof." Each of the rejected claims contains elements as a means for performing specified functions, in accordance with 35 USC 112, and therefore recites a statutory apparatus.

The examiner also contends that the specification describes, on page 8 line 12 through page 9 line 20, the means for retrieving, generating and transmitting as software. That is incorrect. The cited passage is replete with references to a host computer, a hardware token, and a server, all performing certain described functions, but does not describe the means for retrieving, generating and transmitting as software. Furthermore, even if it were true that the

Appln. No. 10/701,029
Reply to non-final Office Action mailed July 24, 2008.

PATENT

cited passage, in addition to explaining the operation and interaction of those various elements, suggested that those functions could alternatively be accomplished purely in software (which it does not), it would be improper for the examiner to import such a limitation from the specification into the claims. MPEP 2111.01 (II).

Based on the remarks presented above, reconsideration and withdrawal of the rejection of claims 49, and 51-63 under 35 USC § 101 are respectfully requested.

Claim Rejections - 35 USC § 103

Claims 34-35, 38-44, 49-50, 53-59, 64-65, and 68-74 stand rejected under 35 USC § 103(a) as being allegedly unpatentable over Iijima (US Patent 5,225,664) in view of Ho et al. (US PG Pubs 20030143989 A1). Applicant respectfully traverses this rejection in connection with the claims as now presented.

The claims are directed to preventing unauthorized access to a secure computing environment protected by a hardware token, in the event an unintended user acquires the token (such as by stealing it or finding a token that was lost by its intended user) and tries to access the system with it. One (or more) specific host computer(s) are set up to work in conjunction with the token, by storing on the host a non-varying value X that is based on an identifier P securing access to the token, combined with a non-varying computer fingerprint F of the host. The fingerprint F is computed from non-varying host information C based on a unique characteristic of the host, such as hardware information like a serial number of a host processor or hard drive, a NIC MAC address, or the like. The fingerprint of the host is not stored in the token, and the token cannot thereafter be used to gain access to the secured computer system or data except in conjunction with the host(s) it is set up to work with.

Iijima's authentication requires the use of random numbers, and it requires that the host terminal and the IC card are mutually authenticated to each other. In contrast, in the claims no random numbers are used, and only one device is authenticated to work with the other. The two methods cater to different needs—authentication using random numbers as in Iijima can be used to prevent replay attacks; while the claims prevent unauthorized access involving use of a stolen or lost token.

In Iijima, during a setup process "generated random number information B [is encrypted] by using ... internal data NNNNN as an encryption key, and the result is stored into a preset area of the internal RAM [of the IC card] as authentication information C2X" (Iijima, column 4 lines 43-47). The "random number information B" and an indicator of internal data NNNNN are then sent to the terminal (where they presumably must be stored for later authentication of the token). During authentication, "an encryption of random data B using key data NNNNN is executed in the terminal 8 to obtain an encrypted data C2 which is then transmitted to the IC card 1.... [A]uthentication information C2 ... and authentication information C2X stored in the internal RAM [of the IC card] are compared with each other" (Iijima, column 4 line 61-column 5 line 1). A similar process is also performed reversing the roles of the IC card and the terminal, wherein an encryption of random data A is performed using key data MMMMM in the IC card to obtain encryption data C1. C1 is transmitted to terminal 8, where authentication information C1X is generated in terminal 8 and compared with C1 (Iijima, column 5 lines 6-21). "By this flow control, the mutual authentication of the IC card with the terminal device 8 can be attained" (Iijima, column 5 lines 22-23).

Regarding claims 34, 49, and 64, those claims recite authentication comprising retrieving a non-varying value X from a memory separate from the token generated in part from an

identifier P securing access to the token, from which P is regenerated and sent to the token. A somewhat analogous operation in Iijima is authentication comprising the retrieval of random number B and key data NNNNN for generating C2, which is sent to the IC card. Several differences between the claims and Iijima are apparent. In the claims, a non-varying value X is retrieved. X was generated in part from a non-varying computer fingerprint F of the host, which was computed using non-varying host information C based on a unique characteristic of the host (such as a processor or hard drive serial number, NIC MAC address, or the like). The examiner contends that Iijima discloses retrieving such a value X, and equates the value X of the claims with the value C2X of Iijima. However, C2X is not retrieved from a memory separate from the token for authentication, as in the claims. Instead, C2X is generated from random number information B and key data NNNNN.

In addition, in the claims the value X is generated from a non-varying computer fingerprint F of the host, calculated from non-varying host information C. The examiner contends that NNNNN can be identified with fingerprint F, but that is incorrect. The portions of Iijima cited by the examiner on this point (column 3 lines 64-67, column 4 lines 21-26, and column 4 lines 42-50) do not make clear the source of internal data NNNNN, but seem to indicate that it includes "a number which is inherent to the card [but not to the host] and set when the card is issued" (Iijima column 4 lines 23-25). Iijima, column 7 lines 14-27 sheds further light on this: "data used as the basis for generation of the random number information is read out from the data memory of the card and newly generated random number information is stored in the data memory so as to be used as data which can be used as the basis for generation of the next random number information. Further, at the time of issuing the card, designated data such as card inherent number stored in the data memory is set as a parameter for generation of random

number information. As a result, even when the same random number information items are input to the IC card, different data can be generated in each time and different data can be generated in different IC cards" (emphasis added). Thus, the "card inherent number" appears to be simply an arbitrary value stored in a memory of the card to be used as a first value for generating random number information, which replaces the first value in the memory and in turn is used to generate new random information when needed, and so on. It is not related to the non-varying host information C that is based on a unique characteristic of the host, from which a non-varying host fingerprint F is computed.

The examiner admits that Iijima fails to disclose regenerating the same identifier value P from the value X and the host fingerprint F, and transmitting the regenerated identifier P, and relies on Ho only for that feature. However, Ho is not directed to an authentication process, and does not supplement Iijima to provide the features not found therein discussed previously. Instead, Ho is directed to synchronization of stored service parameters. A configuration identifier is transmitted from a mobile station to a base station, and compared with an identifier generated in the base station. If the identifiers match, the configuration may be used for the call. The benefit of Ho is that it avoids attempted use of unsynchronized stored service parameters and associated call setup failures and subsequent renegotiation, thereby reducing call setup time. That has nothing to do with using non-varying host computer information to authenticate a token.

Thus it can be seen that Iijima and Ho, alone or in any possible combination, do not disclose, suggest, or render obvious authenticating a hardware token for operation with a host, comprising retrieving a non-varying value X from a memory separate from the token, generated from a non-varying computer fingerprint F of the host and an identifier P securing access to the

Appln. No. 10/701,029
Reply to non-final Office Action mailed July 24, 2008.

PATENT

token, wherein F is computed from non-varying host information based on a unique

characteristic of the host, as recited in claims 34, 49, and 64. Therefore, the rejection of those

claims under 35 USC § 103(a) is not supported, and they are deemed allowable over the cited

prior art. Claims 38-44 depend from claim 34, claims 53-59 depend from claim 49, and claims

68-74 depend from claim 64, and those claims are deemed allowable for at least the same

reasons as their base claims.

Based on the arguments presented above, reconsideration and withdrawal of the rejection

of claims 34, 38-44, 49, 53-59, 64, and 68-74 under 35 USC § 102(b) are respectfully requested.

Claims 45-48, 60-63, and 75-78 stand rejected under 35 USC § 103(a) as being allegedly

unpatentable over Iijima (same as above) and Ho (same as above) in view of Miura (US Patent

No. 6,952,775). Claims 36-37, 51-52, and 66-67 stand rejected under 35 USC § 103(a) as being

allegedly unpatentable over Iijima (same as above) and Ho (same as above) in view of Ayyagari

et al. (US 2003/0208677). Applicant respectfully traverses these rejections.

Claims 45-48, 60-63, and 75-78 depend from claims 34, 49, and 64, respectively, and it is

noted that Miura is relied on only for the additional features of claims 45-48, 60-63, and 75-78.

Miura does not supplement Iijima combined with Ho to provide the elements of claims 34, 49,

and 64 missing therefrom. Therefore, without prejudice to their own individual merits, claims

45-48, 60-63, and 75-78 are deemed allowable over the cited references for at least the same

reasons that claims 34, 49, and 64 are allowable over Iijima combined with Ho.

Claims 36-37, 51-52, and 66-67 also depend from claims 34, 49, and 64, respectively,

and it is noted that Ayyagari is relied on only for the additional features of claims 36-37, 51-52,

and 66-67. Ayyagari does not supplement Iijima and Ho to provide the elements of claims 34,

Appln. No. 10/701,029
Reply to non-final Office Action mailed July 24, 2008.

PATENT

49, and 64 missing therefrom. Therefore, without prejudice to their own individual merits, claims 36-37, 51-52, and 66-67 are deemed allowable over the cited references for at least the same reasons that claims 34, 49, and 64 are allowable over Iijima combined with Ho.
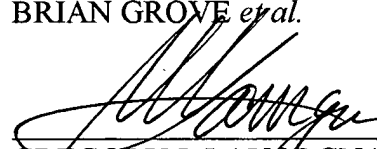
Conclusion

In view of the foregoing amendment and remarks, Applicants respectfully submit that claims 34, 36-49, 51-64, and 66-78 are in condition for allowance and a notice of allowance is respectfully requested.

Respectfully submitted,

BRIAN GROVE *et al.*

BY:

GREGORY J. LAVORGNA
Registration No. 30,469
Drinker Biddle & Reath LLP
One Logan Square
18th and Cherry Streets
Philadelphia, PA 19103-6996
Tel: 215-988-3309
Fax: 215-988-2757
Attorney for Applicant